MoqHao Part 1: Identifying Phishing Infrastructure

team-cymru.com/blog/2021/01/20/moqhao-part-1-identifying-phishing-infrastructure/

S2 Research Team View all posts by S2 Research Team January 20, 2021

Domain
t.aeodr.com
t.aeogu.com
t.aeoin.com
t.aeokc.com
t.aeomc.com
t.aeomg.com
t.aeomh.com
t.aeomk.com
t.aeomnv.com
t.aeomp.com
t.aeomq.com
t.aeomt.com
t.aeomu.com
t.aeomz.com
t.aeoob.com
t.aeovn.com
t.aeoxi.com
t.aeoxq.com
t.aeoyhl.com

In mid-January, Twitter users @NaomiSuzuki_ and @KesaGataMe0 identified nearly 20 malicious phishing domains spoofing AEON Bank in Japan. The domains were tied to MoqHao, a malware family targeting Android OS devices, primarily in Japan, South Korea, and Taiwan:

Domain
t.aeodr.com
t.aeogu.com
t.aeoin.com
t.aeokc.com
t.aeomc.com
t.aeomg.com
t.aeomh.com
t.aeomk.com
t.aeomnv.com
t.aeomp.com
t.aeomq.com
t.aeomt.com
t.aeomu.com
t.aeomz.com
t.aeoob.com
t.aeovn.com
t.aeoxi.com
t.aeoxq.com
t.aeoyhl.com

Figure 1 – Seed Twitter Post

Passive DNS Data

Using Team Cymru's Pure Signal Platform, we performed a wildcard search for domains using the pattern of 't.aeo*.com'. This search identified all of the domains and the hosting IP addresses previously found by @NaomiSuzuki_ and @KesaGataMe0.

IP Address	AS Name	Hostname	First Seen
103.75.189.31	Gigabit Hosting, MY	t.aeokc.com	2021-01-07
103.75.189.31	Gigabit Hosting, MY	t.aeomnv.com	2021-01-07
104.27.180.110	Cloudflare, US	t.aeogu.com	2021-01-11
104.27.180.110	Cloudflare, US	t.aeogu.com	2021-01-11
104.27.188.38	Cloudflare, US	t.aeoin.com	2021-01-11
104.27.188.38	Cloudflare, US	t.aeoin.com	2021-01-11
172.67.199.42	Cloudflare, US	t.aeogu.com	2021-01-11

172.67.215.77	Cloudflare, US	t.aeoin.com	2021-01-11
178.132.7.109	WorldStream, NL	t.aeomk.com	2021-01-15
188.213.49.231	Parfumuri Femei, RO	t.aeomq.com	2021-01-13
20.48.114.7	Microsoft, US	t.aeomk.com	2021-01-15
20.48.114.7	Microsoft, US	t.aeomp.com	2021-01-14
20.48.114.7	Microsoft, US	t.aeomz.com	2021-01-15
213.183.48.212	Melbicom, LT	t.aeoyhl.com	2021-01-08
216.189.159.35	HostUS, US	t.aeokc.com	2021-01-07
216.189.159.35	HostUS, US	t.aeomnv.com	2021-01-07
216.189.159.35	HostUS, US	t.aeovn.com	2021-01-08
27.100.36.35	HostUS, AU	t.aeomnv.com	2021-01-07
40.74.72.100	Microsoft, US	t.aeomt.com	2021-01-12
40.74.72.100	Microsoft, US	t.aeoob.com	2021-01-11
45.121.147.170	Gigabit Hosting, MY	t.aeoin.com	2021-01-11
45.121.147.170	Gigabit Hosting, MY	t.aeomg.com	2021-01-14
45.121.147.170	Gigabit Hosting, MY	t.aeomh.com	2021-01-15
45.121.147.170	Gigabit Hosting, MY	t.aeomu.com	2021-01-13
45.121.147.242	Gigabit Hosting, MY	t.aeomc.com	2021-01-15
45.121.147.242	Gigabit Hosting, MY	t.aeoxq.com	2021-01-18
45.121.147.50	Gigabit Hosting, MY	t.aeodr.com	2021-01-08
45.121.147.50	Gigabit Hosting, MY	t.aeoxi.com	2021-01-08
45.58.52.60	HostUS, US	t.aeodr.com	2021-01-08
45.58.52.60	HostUS, US	t.aeoyhl.com	2021-01-08
51.83.247.167	OVH, FR	t.aeoxq.com	2021-01-18

Table 1 – Domains Spoofing Aeon Bank

From this list we can see that several of the IP addresses were used to host two or more domains:

IP Address	AS Name
45.121.147.50	Gigabit Hosting, MY
45.58.52.60	HostUS, US
103.75.189.31	Gigabit Hosting, MY
216.189.159.35	HostUS, US
45.121.147.242	Gigabit Hosting, MY
45.121.147.170	Gigabit Hosting, MY
20.48.114.7	Microsoft, US
40.74.72.100	Microsoft, US

Table 2 – IP Addresses Hosting Multiple Phishing Domains

Performing a passive DNS search on these IP addresses identifies another pattern of spoofed domains, this time targeting Japan's The 77 Bank, Ltd.

By performing another wildcard domain search for '77*bnk.com' we identified the following:

IP Address	AS Name	Name Queried	Min of Timestamp
103.75.189.31	Gigabit Hosting, MY	77cbnk.com	2021-01-07
104.27.180.251	Cloudflare, US	77ebnk.com	2021-01-12
104.27.181.251	Cloudflare, US	77ebnk.com	2021-01-12
172.67.158.54	Cloudflare, US	77ebnk.com	2021-01-12
216.189.159.35	HostUS, US	77obnk.com	2021-01-08
27.100.36.35	HostUS, AU	77bbnk.com	2021-01-05
27.100.36.35	HostUS, AU	77cbnk.com	2021-01-06

Table 3 – Domains Spoofing The 77 Bank

Several of these domains, including 77cbnk.com, 77bbnk.com, and 77bac.com were already observed by Twitter sleuths @NaomiSuzuki_ and @KesaGataMe0.

Note: A domain spoofing Japan's Jibun Bank, 't.auznw.com' was also hosted on 45.121.147.242, but we couldn't find any more domains that followed the same pattern. Likewise, the domains 'aetvk.com', 'aenbv.com', 'aeenm.com', and 'aenvv.com' were also

used to spoof AEON Bank (using a slightly different naming pattern) but did not lead to any additional discoveries.

X.509 Data

Looking at our X.509 certificate records, we find one certificate hosted on IP address 40.74.72.100:

Field	Value
Subject DN	CN=aeoob.com
Issuer DN	C=US, O=Let's Encrypt, CN=R3
Serial	0xeeb4ec0ef406cb854ddffb1c9fd2276c
Validity	2021-01-11 07:49:38 to 2021-04-11 07:49:38 (90 days)
SHA-1	c2029fa68bfa34fefc4ac48360434989122f1348

Table 4 – x509 Certificate Associated with aeoob.com

None of the other domains appeared to have an associated certificate, so it is unknown why the domain 'aeoob.com' is the exception. Nonetheless, it's an additional data point to look out for in the future.

NetFlow Data

Looking at netflow, we see over 250 unique Japanese IP addresses connecting over TCP port 443 (HTTPS) to the IP addresses in Table 2. The connecting IP addresses are all registered to Softbank, NTT, OPTAGE, or NTT Docomo, indicating they are likely residential customers. The vast majority of overall TCP/443 traffic to these IP addresses came from Japan, so the traffic likely represents victims who fell prey to the phishing campaign.

The actors appear to have covered their tracks carefully. A high percentage of the netflow traffic directed at five of the eight IP addresses listed in Table 2 came from 210.140.10.24 (IDC Frontier Inc., JP) and 45.114.130.4 (EHOSTIDC, KR), both of which are Tor exit nodes.

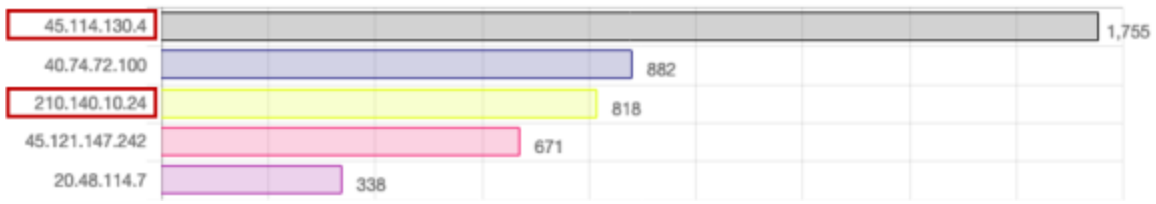

Figure 2 – Top Communicating IP Addresses in NetFlow Data

While we can’t draw any further conclusions as to attribution of this activity at this stage, with Team Cymru’s Pure Signal platform we can continue to monitor new spoofed banking domains and IP addresses as they appear.